JOHN EMMERSON BATTY PRIMARY SCHOOL

"Aim High, Reach for your Goal"

John Emmerson Batty Primary School

E-Safety Policy and Acceptable Use of ICT Agreements 2018

1. Introduction

At John Emmerson Batty Primary School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

John Emmerson Batty Primary School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools

- policies and procedures, with clear roles and responsibilities

- a comprehensive e-safety programme for pupils, staff and parents.

This policy has been contributed to by the whole school and ratified by the governors.

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Safeguarding Policy and Child Protection Policy, Code of Conduct policy and Equal Opportunities Policy.

Introduction of E-Safety Policy and whole school community involved including pupils.

Whole school E-Safety training took place throughout September 2017

2. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in John Emmerson Batty Primary School. All staff on the Child Protection team have received CEOP (Child Exploitation and Online Protection) training.

Martin Kitchen (Head teacher) has overall responsibility. Julie Norris (DHT/Computing Lead) is the named member of staff for children to report any concerns.

It is the role of the computing lead to keep abreast of current issues and guidance through organisations such as Redcar and Cleveland LA, Becta, CEOP (Child Exploitation and Online Protection), and Child Net. The Head teacher ensures Senior Management and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- safe use of the Internet
- safe use of the school network, equipment and data including the safe use of school and home e-mail
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community (see appendix 5)
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. All staff, including Supply Teachers/Governors, must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 4 for staff acceptable use agreement).

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- E-safety posters will be prominently displayed.

3. Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety.

- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the Computing curriculum.
- We regularly distribute questionnaires to children to monitor their understanding of e-safety. Please see Appendix 6. Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

4. Managing Internet Access

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor RCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Our internet access is controlled through the Local Authority (10Mb Broadband)

5. How will information systems security be maintained?

- Users must take responsibility for their network use.
- Servers are located securely and physical access restricted.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LA
- Access by wireless devices is pro-actively managed.
- All Internet connections are arranged via the school's 10Mb broadband connection, which is provided by the Local Authority. This in turn links into the Northern Grid network and ultimately the National Education Network. The filters at each stage are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments.
- However, when dealing with the internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined below have been taken.
- Files held on the school's network will be regularly checked.
- The Computing leader/LA ICT technician will review system capacity regularly.
- Pupils will inevitably access the internet outside of school. We therefore aim to educate them about internet safety, not simply cover their eyes.

6. How will e-mail be managed?

Pupils

Pupils from Year 4, 5 and 6 will be given a "professional" email account. The account is set up through Office 365. The pupils are at liberty to use their accounts for correspondence between anyone registered on the jebatty.rac.sch.uk domain. They must ask a member of staff before using it to contact or reply to anyone else not registered as a user on the J.E. Batty

Learning Platform. Passwords will be issued by the subject leader/ICT technician. Users agree through the home/school Computing and E-

Safety, Acceptable Use agreement form to keep passwords secret from anyone else apart from the Computing subject leader and their parents.

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- The forwarding of chain letters is not permitted.

The email system has a powerful filter which will automatically direct emails with inappropriate language to the administrator account. This account will be checked through the forwarding of inappropriate mail to the Head Teacher's professional email account. The Head Teacher will also monitor internet/e-mail use every week to ensure it continues to be used appropriately.

- Use of personal email accounts by pupils in school is not permitted.
- Use of newsgroups, forums, chat-rooms or social networking sites, by pupils in school, is not permitted unless located on the learning platform.

All of the above information is found in the home/school agreement which must be signed by both the parent/guardian and the child **before** a user account is allocated. Failure to adhere to the agreement will result in suspension of access rights to the internet for the individual child until the agreement is signed up to.

Staff

Staff will be given a "professional" email account. The account is set up using Office 365. The staff are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work. Passwords must be changed. Users agree through the staff computing and E-Safety Acceptable Use agreement form, to keep passwords secret, even from their family and friends.

The email system has a powerful filter which will automatically direct emails with inappropriate language to the administrator account. This account will be checked through the forwarding of inappropriate mail to the Head Teacher's professional email account. The Head Teacher will also monitor internet/e-mail use every week to ensure it continues to be used appropriately.

- Users will also be expected to report any offensive emails that they receive to a Senior Team Leader.

- Any intercepted emails or reports of offensive emails will be reported to the Head Teacher.
- The Head Teacher and system Administrator will have the right to have access to all staff member's professional email accounts.
- Use of personal email accounts in school is permitted only in circumstances where this is done in the staff's own time and using own network (e.g. lunch time).
- Use of personal email accounts in dedicated teaching time is not permitted in any circumstance.
- Use of newsgroups, forums, chat-rooms or social networking sites in school is not permitted unless located during staff's own time, using their own network and in staff room (e.g. lunch time, after school).

The staff internet agreement form sets out the terms and conditions that they must agree to **before** being allocated an account. Failure to adhere to the agreement will result in suspension of internet access rights for the individual and may result in disciplinary measure being taken by the governing body.

Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator and an email sent to the network manager so that they can block the site.

It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering must be authorised by a member of the senior leadership team.

7. Emerging and Wireless Technologies

Management

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out using the LA checklist (See Appendix 6) before purchase and use in school is allowed.
- Mobile phones will not be allowed in school, to be used during lessons or formal school time by pupils, but may be used by staff during staff non-teaching/personal time (E.g. breaks and lunchtime).

Wireless Network security

- The school's wireless network is encrypted by the school ICT technician through Redcar and Cleveland LA provided by the ICT Service Level Agreement, so as to prevent unauthorised access.
- It has been checked and authorised by the LA network administration team.
- If a breach in security is discovered it will be reported to the Head Teacher and steps will be taken to review the security level in place with relevant specialists.
- Accidental access to inappropriate material will be reported on the Computing accidental access chart kept in the Computing suite. This will be monitored on a daily basis by the school computing support technician
- Staff are permitted to access their personal wireless connection to the internet at their place of residence, but no user should attempt to use the school's computing equipment to access any network other than the school's network or personal home network.

Use of mobile devices

- Pupils are not permitted to have mobile phones in school. Failure to observe this will result in confiscation.
- Use of mobile phones by parents and other visitors when in school is permitted only when they are outside of the building.
- Use of mobile phones by staff in school is permitted only in circumstances where this is done during non-teaching/non-contact/personal time.
- Use of mobile phones during dedicated teaching time, or during staff meetings is not permitted in any circumstance. Mobile phones should be switched off or set to silent during these times.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, the school brochure and on the school website.
- School seek the views of parents on the policy on a regular basis using annual parent/carer surveys and through the provision of information within the fortnightly newsletter and the learning platform.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Any parent / carer concerned about the use or teaching of computing in school should contact the Computing Leader in the first instance. The Computing leader will then liaise as appropriate with other staff members and the Head Teacher in an attempt to engage with these concerns.
- Where a parent/carer has a complaint about any use of computing within school the school's complaints policy should be adhered to.
- The views of any parents/carers with specific religious beliefs on the use of technology will be considered.

7. Admin Network

The school adheres to the LA policy regarding use of the administration machines.

8. Security and Data Protection

- Use of the network for personal monetary profit or gambling is strictly forbidden.
- In accordance with the Data Protection Act 1984/98, users are not allowed to access other user's personal files and folders. The exception to this being system administrators who can gain access through permission from the Head Teacher when just cause has been established.
- Staff are made aware of LA Guidelines for data protection through LA documentation sent to all LA employees. (Copy kept in E-Safety box held in computing suite)
- A copy of the LA Safeguarding document is also made available to staff for reference and a copy is kept on the school's learning platform for agreed users to access. (Copy in E-Safety box in computing suite.)
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy.

9. E-Safety Complaints/Incidents

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may means that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Head teacher. Incidents should be logged and the policy for managing an e-safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying

and children, staff and families need to know what to do if they or anyone they know are a victim of Cyberbullying. All bullying incidents should be recorded and investigated via the incident log form **(Appendix 5)**.

10. Review of Policy

There are on-going opportunities for staff, children and families to discuss e-safety concerns with our staff. This policy needs to be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or any guidance or orders are updated.

Appendix

1. Parent Internet use form/letter
2. Primary Pupil Acceptable Use of ICT Agreement
3. Pupil E-Safety Rules
4. Staff, Governor and Visitor Acceptable Use Agreement
5. E-Safety Incident Log
6. Emerging Technologies Risk Assessment
7. KS2 E-safety questionnaires
8. KS1 Internet tips (8a -8b)
9. KS2 Internet tips (9a – 9b)
10. Internet Safety – Snakes and Ladders game
11. Possible Teaching and Learning Experiences

Policy agreed by the governing body on 10th December 2018

Signed:

Reviewed: **December 2018** **By:** **J Norris**